wandera
a Jamf company

# Threat Defense

**Proteja sus dispositivos, usuarios y aplicaciones de amenazas cibernéticas con una seguridad basada en la nube que opera en el dispositivo y la red.**

## Seguridad de endpoints (puntos finales) garantizada

Threat Defense detecta y resuelve una gran gama de amenazas de endpoints (puntos finales), incluyendo las vulnerabilidades de dispositivos, el malware y las aplicaciones de riesgo. Se llevan a cabo evaluaciones de riesgo integrales de manera continua para detectar amenazas y aplicar políticas de seguridad en tiempo real.

## Las defensas de la red protegen a usuarios y datos

Detenga los ataques antes de que afecten las defensas de la red. La protección de contenidos bloquea los sitios maliciosos, aunque se trate de sitios de phishing nunca antes vistos (desde día cero) diseñados para robar credenciales corporativas. Además, Threat Defense evita el control de comandos y la filtración de datos al bloquear la conectividad a sitios de riesgo. Cuando se detectan ataques al intermediario, las conexiones quedan protegidas automáticamente.

## Acceso adaptable a sus aplicaciones

Eleve su postura de seguridad permitiendo únicamente el acceso de dispositivos seguros y de confianza a las aplicaciones de empresa. Threat Defense monitorea continuamente un amplio conjunto de datos de telemetría y contextuales que pueden usarse para impedir el acceso a las aplicaciones cuando un endpoint (punto final) está comprometido o presenta un alto riesgo. Las políticas de acceso adaptables pueden aplicarse de manera nativa mediante la solución Zero Trust Network Access o la solución de gestión de Jamf, Jamf Pro.

# Detección y prevención integral de amenazas

Threat Defense identifica y detiene una amplia gama de amenazas cibernéticas

### Protección de red en tiempo real

Threat Defense detecta y bloquea dinámicamente los intentos de robo de credenciales de usuario para garantizar que incluso los ataques de phishing desconocidos no logren su cometido. Se escanean una amplia gama de factores, como la imitación de marcas, punycodes (código púny) sospechosos y entropías de subdominio. La protección inherente a la red rechaza los ataques enviados por correo electrónico, redes sociales y SMS.

### Detección de configuraciones de riesgo

Las evaluaciones de postura detalladas ofrecen a las organizaciones visibilidad acerca de los riesgos de endpoints (puntos finales), desde privilegios no autorizados hasta sistemas operativos anticuados. Los controles granulares permiten la aplicación de políticas de seguridad a través de medidas de remediación, como avisos a los usuarios finales, el bloqueo de conexiones maliciosas y el acceso restringido a recursos corporativos.

### Información detallada sobre aplicaciones

Comprenda los riesgos de cada aplicación de un solo vistazo, tenga plena visibilidad de las vulnerabilidades conocidas con la puntuación de riesgo de aplicaciones de MI:RIAM y considere las acciones de remediación recomendadas. Podrá consultar datos forenses detallados para entender las autorizaciones requeridas, las URL o las bibliotecas de terceros usadas por versiones específicas de una aplicación.

### Prevención de interceptaciones de comunicaciones

Las conexiones de Wi-Fi públicas son plataformas muy atractivas para los agentes maliciosos. Threat Defense protege dispositivos conectados a Wi-Fi con cifrado Failsafe. Cuando se detecta un ataque, Threat Defense cifra automáticamente el tráfico del usuario para que este pueda seguir trabajando de manera segura sin interrupciones de conexión.

# Características y capacidades de seguridad líderes

Protección sólida para todos los casos de uso y compatibilidad con cualquier sistema

### Defensa de endpoints siempre activa

Proteja a los usuarios y dispositivos de las ciberamenazas estén donde estén. La aplicación para endpoints de Wandera detecta software maliciosos, configuraciones vulnerables y conexiones de alto riesgo antes de que se produzca el ataque. Las acciones y alertas de corrección se activan automáticamente para mitigar posibles amenazas.

### Informes y control de políticas en tiempo real

El motor de políticas unificadas permite a los administradores configurar rápidamente una política de seguridad. La aplicación y cumplimiento de las políticas entran en vigor de inmediato, y todas las políticas pueden irse modificando y ajustándose sobre la marcha. Pueden consultarse datos detallados en todo momento desde el portal de Threat Defense o en un panel SIEM/SOAR (que podrá integrar como solución lista para usar o con una suite de API y datastreams).

### Políticas de acceso condicional con Conditional Access

Evite que usuarios o dispositivos de riesgo tengan acceso a las aplicaciones empresariales con Conditional Access. Los permisos de dispositivos BYOD tanto gestionados por la empresa como no gestionados por la empresa quedarán revocados hasta que vuelvan a clasificarse como seguros. Las políticas pueden aplicarse nativamente dentro de la red de Threat Defense o a través de una integración con Jamf o IdP.

### Operaciones y gestión unificados

Al integrar Threat Defense con una solución de gestión como Jamf o IdP, podrá sincronizar los datos sobre los grupos de usuarios de la organización. Así, podrá implementar Threat Defense en los dispositivos de los usuarios rápidamente y las asignaciones de permisos por usuario serán mucho más sencillas. Esta integración también simplifica los procesos de control de eventos y búsqueda de amenazas de ThreatOps, ya que agrega nombres humanos legibles a los informes.

## Tecnología MI:RIAM

MI:RIAM es un motor de inteligencia de amenazas; funciona en tiempo real para identificar una amplia variedad de amenazas conocidas y desde el día cero. Basada en el mayor conjunto de datos de amenazas, MI:RIAM recoge información de 425 millones de sensores de todo el mundo para calcular sus algoritmos. MI:RIAM utiliza la ciencia de datos más avanzada para proporcionar a los directores de seguridad datos en tiempo real de la inteligencia de amenazas y sobre riesgos activos para la empresa.

Para obtener más información sobre cómo Threat Defense protege a usuarios, dispositivos móviles y datos corporativos de intenciones maliciosas, visite jamf.com.

wandera
a Jamf company